

INSTRUCTIONS FOR THE CG-6025

FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY

This form satisfies the requirements for Facility Vulnerability and Security Measures Summary submission found in the Code of Federal Regulations for Facility Security. Form CG-6025A, Vulnerability and Security Measures Addendum, may be used as a continuation of form CG-6025, in order to submit additional vulnerabilities and security measures. If a facility owner or operator submits a Facility Vulnerability and Security Measures Summary pertaining to more than one facility, form CG-6025, shall be submitted to document each additional facility.

BLOCK 1	Self-Explanatory.	BLOCK 8b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 2	Street Address.		
BLOCK 3	If available, provide latitude to nearest tenth of a minute.		
BLOCK 4	If available, provide longitude to nearest tenth of a minute.	BLOCK 9a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 2 that will mitigate the vulnerability you addressed.
BLOCK 5	Provide the Captain of the Port Zone from the list below in which your facility resides. Their respective zones are described in 33 CFR Part 3.	BLOCK 9b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 6	Check all applicable operations that are conducted at your facility. If you select other, please explain in the box provided.		
BLOCK 7a	Enter a concise description of a vulnerability identified in your facility's assessment. Provide location information if appropriate.	BLOCK 10a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 3 that will mitigate the vulnerability you addressed.
BLOCK 7b	Enter the vulnerability identification code from the KEY to categorically identify the vulnerability you described. More than one category may be used. If you select other, please explain in the box provided.		
BLOCK 8a	Enter a concise description of a selected security measure identified in the plan for MARSEC Level 1 that will mitigate the vulnerability you addressed.	BLOCK 10b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.

CAPTAIN OF THE PORT ZONE:

Anchorage	Honolulu	Mobile	Puget Sound
Baltimore	Houston-Galveston	Morgan City	San Diego
Boston	Huntington	New Orleans	San Francisco
Buffalo	Jacksonville	New York	San Juan
Charleston	Juneau	Paducah	Sault Ste. Marie
Chicago	Long Island Sound	Philadelphia	Savannah
Cleveland	Los Angeles/Long Beach	Pittsburgh	St. Louis
Corpus Christi	Louisville	Port Arthur	Tampa
Detroit	Memphis	Portland, ME	Toledo
Duluth	Miami	Portland, OR	Valdez
Guam	Milwaukee	Providence	Wilmington
Hampton Roads			

KEY

VULNERABILITY CATEGORY:

Physical Security	PHS	That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against terrorism, espionage, sabotage, damage, and theft.
Structural Integrity	STI	The design and material construction characteristics of piers, facilities, and associated structures.
Transportation Infrastructure	TRI	Infrastructure that may be exploited during an attack, other than utilities.
Utilities	UTI	The essential equipment and services that are vital to the operation of the facility.
Radio & Telecommunications	RAT	That part of security concerned with measures to protect radio and telecommunication equipment, including computer systems and networks.
Personnel Protection Systems	PPS	Equipment, Gear, or Systems designed to protect facility personnel (i.e. weapons, body armor, masks).
Procedural Policies	PRP	Plans, Policies, and Procedures for specific operations.
Coordination and Information Sharing	CIS	The ability to coordinate and receive/share information with local/state/federal agencies and other commercial entities.
Preparedness	PRE	Implementation of Plans, Policies, and Procedures through Training, Drills, and Exercises conducted to improve security awareness, prevention, and response.

SECURITY MEASURES

Access Control	ACC	Lighting	LIT
Barriers	BAR	Patrols	PAT
Cargo Control	CAC	Planning, Policies, & Procedures	PPP
Communications	COM	Redundancy	RED
Coordination	COR	Response	RES
Credentialing	CRE	Stand-off Distance	SOD
Detection	DET	Structural Hardening	STH
Guard Force	GUF	Surveillance	SUR
IT Security	ITS	Training	TRA
Inspections	INS	Vessels/Vehicles	VEV
Intelligence	INT		